Section III:

AMENDMENT UNDER 37 CFR §1.121 to the DRAWINGS

No amendments or changes to the Drawings are proposed.

Section IV:

AMENDMENT UNDER 37 CFR §1.121

REMARKS

Summary of Telephone Interview

On May 17, 2005, Applicant's Agent, Robert H. Frantz, Examiner Dada and Primary Examiner Ho Fong held a telephone interview at the applicant's request to discuss a proposed amendment provided by applicant's agent in advance of the interview.

Applicant's agent explained applicant's understanding or interpretation of Crosbie's published patent application 2002/0083343 A1 (hereinafter "Crosbie") as teaching a single rule relating to detecting potential hacker threats via use of a UNIX switch-user ("SU") command. This rule looks for a number N of failed SU commands in a configurable period of time starting at the first failed command to the N^{th} attempt. If more failed attempts are made during this time, an alert is generated. Crosbie's paragraphs 0345 - 0343 teaches this logic applied to the SU command, and teaches similar logic applied to the LOGIN command at paragraphs 0335 - 0339. The examiners did not have any disagreement with this understanding of Crosbie's disclosure.

Next, applicant's agent briefly explained the differences in applicant's invention with reference to the proposed claim amendments:

(a) that applicant's *plurality* of different logical rules are configurable and are included in a *single* file, where Crosbie's *singular* rule is stored in a separate template from their other security measures, which allows our multiple-logic-rule implementation to be easy to manage and configure;

(b) that applicant's rules include several logic rules or conditions beyond Crosbie's N-failures-in-T-time:

(1) produce an alert when *anyone* switches to a specified user ID, which Crosbie doesn't teach;

(2) produce an alert when *anyone* switches to a specified the ROOT UID, which Crosbie doesn't teach;

(3) produce an alert when *anyone* switches to *any* other user ID during a specified period of time, which Crosbie doesn't teach; and

(c) that applicant's rules include a configurable parameter to send an alert message via e-mail to an address designated in the rules file, which Crosbie does not teach.

The examiners agreed that the proposed amendment would overcome the art of record, but additional searching may be needed before making an allowance of the claims.

Rejections Under 35 U.S.C. §102(e)

Rejections of Claims 1 - 16 Over Crosbie

In the Office Action, claims 1 - 16 were rejected under 35 U.S.C. §102(e) as being anticipated by Crosbie. Applicant has amended the independent claims such that they recite steps, elements or limitations, and applicant is amending the application to include a number of new claims drawn specifically to the logical rules or processes disclosed by applicant, none of which are taught by or suggested by Crosbie, as agreed upon during the interview.

Further, we have modified the language of the proposed amendment to specify that applicant's rule set includes a rule besides an number-N-of-failures-in-time_period-T logic *wherein the time period begins upon the first failed SU attempt*. This was not discussed during the interview, but applicant's agent highlighted our rules ability to trap or detect SU attempts during specific hours of operation (e.g. absolute time values such as 12:00 am to 1:00 am) instead of a relative time period (e.g. relative to a first failed attempt time value). As such, we are providing clarifying language in our formal amendment.

For these reasons, applicant requests reconsideration of the rejections, and allowance of the claims as amended.

Respectfully,

Robert Frantz

Agent for Applicant(s)
Robert H. Frantz, Reg. No. 42,553
Tel: (405) 812-5613